(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-523820
(P2004-523820A)
(43)公表日　平成16年8月5日(2004.8.5)

(51)Int.Cl.[7]	F I	テーマコード（参考）
G06F 11/00	G06F 9/06 660N	5B076

審査請求 未請求　予備審査請求 有　（全 46 頁）

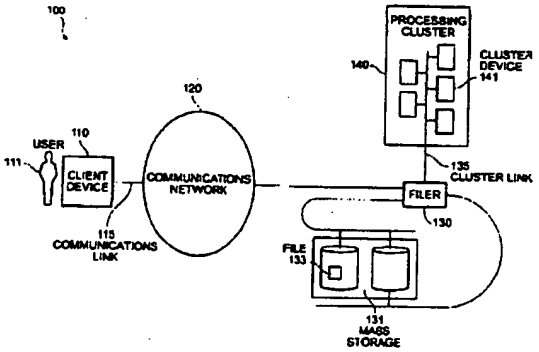
(21)出願番号　特願2002-546962(P2002-546962)
(86)(22)出願日　平成13年11月30日(2001.11.30)
(85)翻訳文提出日　平成15年6月2日(2003.6.2)
(86)国際出願番号　PCT/US2001/046688
(87)国際公開番号　WO2002/044862
(87)国際公開日　平成14年6月6日(2002.6.6)
(31)優先権主張番号　09/728,701
(32)優先日　平成12年12月1日(2000.12.1)
(33)優先権主張国　米国(US)
(81)指定国　EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),CA,JP

(71)出願人　500261341
ネットワーク・アプライアンス・インコーポレイテッド
アメリカ合衆国９４０８９カリフォルニア州サニーベイル、イースト・ジャーバ・ドライブ４９５番
(74)代理人　100086405
弁理士　河宮　治
(74)代理人　100098280
弁理士　石野　正弘
(72)発明者　マーク・ムールスタイン
アメリカ合衆国８５７５０アリゾナ州ツーソン、イースト・プラチタ・アルタ・レポサ５８３１番

Fターム(参考)　5B076 FD08

(54)【発明の名称】分散化された装置でのウィルススキャン

(57)【要約】
特殊なコンピュータ装置をウィルススキャンする方法およびシステムである。好適実施形態にて、ファイラ（１３０）は、エンドユーザへの配信の前にリクエストされたファイルがウィルスフリーであることを確かめる１以上の補助コンピュータ装置（１４０）に接続される。エンドユーザ（１１１）のファイルリクエストにより、以下の工程が実施される。第１に、リクエストファイルをエンドユーザへ送信する前にスキャンしなければならないのか判断する。第２に、ファイラは外部コンピュータ装置の１つ（１４１）へのチャンネルを開き、ファイル名を送る（２０３）。第３に、その外部コンピュータ装置がそのファイルを開いて（２０５）スキャンする（２０７）。第４に、外部コンピュータ装置がファイラへファイルスキャン操作のステータスを報告する（２０９）。第５に、ファイラは、ステータスが送信を許可するならば、ファイルをエンドユーザに送る（２１１）。



BEST AVAILABLE COPY

【特許請求の範囲】
【請求項１】
ファイラを操作する方法であって、
オブジェクトを有する第１ロケーションにおいて、第１通信リンクを介してユーザからの前記オブジェクトに対するリクエストを受け取るステップ、
前記オブジェクトに関する識別子を、第２通信リンクを介して第２ロケーションに送るステップ、
前記第２ロケーションにおける前記リクエストの処理ステップであって、前記処理のステップに少なくとも以下の、
（１）前記オブジェクト内部において１以上の認識可能なデータパターンを検索すること、
（２）前記オブジェクトを圧縮すること、および、
（３）前記オブジェクトを暗号化すること、
のうち１つを含んでいるステップ、
ならびに、
前記リクエストに対する応答ステップであって、前記応答ステップが前記第１通信リンクを介して前記ユーザに対しレスポンスを送信することを含んでいるステップを有する、
ファイラを操作する方法。
【請求項２】
前記リクエストが電子形式で行われる、請求項１に記載の方法。
【請求項３】
前記オブジェクトがファイルである、請求項１に記載の方法。
【請求項４】
前記リクエストの処理ステップがさらに以下の、
前記ファイラから処理クラスタへのアクセスパスを生成するステップ、
前記処理クラスタにおいて前記ファイルを処理するステップ、および、
前記処理クラスタにおいて前記ファイルに関する前記処理に対応したスキャンレポートを作成するステップを含んでいる請求項３に記載の方法。
【請求項５】
前記アクセスパスを生成するステップが、
前記ファイラから前記処理クラスタへ前記ファイルのＩＤおよびパスを送信するステップを有する請求項４に記載の方法。
【請求項６】
前記送信ステップが不均等メモリアクセスを用いて遂行される請求項５に記載の方法。
【請求項７】
前記送信ステップが通信ネットワークを用いて遂行される請求項５に記載の方法。
【請求項８】
前記送信ステップがダイレクト接続を用いて遂行される請求項５に記載の方法。
【請求項９】
前記の、前記ファイルを処理するステップは、前記処理クラスタにより総当り方式で後続の受信ファイルについて実行される請求項４に記載の方法。
【請求項１０】
前記の、前記ファイルを処理するステップは、前記処理クラスタにおける１よりも多い装置により、分けて遂行される請求項４に記載の方法。
【請求項１１】
前記ファイラに記憶されている全てのファイルは論理的に連続的な方式でスキャンされる請求項４に記載の方法。
【請求項１２】
前記スキャンレポートが、前記の、前記ファイルを処理するステップに関する一組のステータスデータを有する請求項４に記載の方法。

【請求項１３】
前記ステータスデータが、前記ファイルにおけるウィルスの存在または非存在を特定する少なくとも１つのデータ要素を含んでいる請求項１２に記載の方法。
【請求項１４】
前記レポートが前記ファイラへ転送される請求項１３に記載の方法。
【請求項１５】
前記レポートが第１データベースに記憶される請求項１４に記載の方法。
【請求項１６】
その後の、前記ファイルに対するスキャンの必要性は、前記データベースが前記ファイルに関するレポートを有するか、および、前記ファイルが最後のアクセスから変更されているかに関する判断による関数である、請求項１５に記載の方法。
【請求項１７】
その後の、前記ファイルに対するスキャンの必要性は、さらなるウィルス識別データファイルが前記処理クラスタに追加されたかに関する判断による関数である、請求項１６に記載の方法。
【請求項１８】
前記レスポンスの送信とは前記ファイルである請求項１に記載の方法。
【請求項１９】
前記レスポンスの送信が、ユーザへの前記ファイルは利用不可能である旨の通知を含む請求項１に記載の方法。
【請求項２０】
前記リクエストに対する応答ステップが、前記ユーザに前記スキャンレポートの写しを送ることを含んでいる請求項１に記載の方法。
【請求項２１】
ファイラを操作するための装置であって、
オブジェクトを有する第１ロケーションにおいて、第１通信リンクを介してユーザからの前記オブジェクトに対するリクエストを受け取るための手段、
前記オブジェクトに関する識別子を、第２通信リンクを介して第２ロケーションに送るための手段、
前記第２ロケーションにおける前記リクエストの処理のための手段であって、前記処理のための手段に少なくとも以下の、
（１）前記オブジェクト内部において１以上の認識可能なデータパターンを検索するための手段、
（２）前記オブジェクトを圧縮するための手段、および、
（３）前記オブジェクトを暗号化するための手段、
のうち１つを含んでいる手段、
ならびに、
前記リクエストに対する応答手段であって、前記応答手段が前記第１通信リンクを介して前記ユーザに対しレスポンスを送信する機能を備えた手段を有する、
ファイラを操作するための装置。
【請求項２２】
前記オブジェクトがファイルである、請求項２１に記載の装置。
【請求項２３】
前記リクエストの処理のための手段がさらに以下の、
前記ファイラから処理クラスタへのアクセスパスを生成するための手段、
前記処理クラスタにおいて前記ファイルを処理するための手段、および、
前記処理クラスタにおいて前記ファイルに関する前記処理に対応したスキャンレポートを作成するための手段を含んでいる請求項２２に記載の装置。
【請求項２４】
前記アクセスパスを生成するための手段が、

前記ファイラから前記処理クラスタへ前記ファイルのＩＤおよびパスを送信するための手段を有する請求項２３に記載の装置。
【請求項２５】
前記送信が不均等メモリアクセスを用いて遂行される請求項２４に記載の装置。
【請求項２６】
前記送信が通信ネットワークを用いて遂行される請求項２４に記載の装置。
【請求項２７】
前記送信がダイレクト接続を用いて遂行される請求項２４に記載の装置。
【請求項２８】
前記の、前記ファイルに対する処理は、前記処理クラスタにより総当り方式で後続の受信ファイルについて実行される請求項２３に記載の装置。
【請求項２９】
前記の、前記ファイルに対する処理は、前記処理クラスタにおける１よりも多い装置により前記ファイルの極小単位に遂行される請求項２３に記載の装置。
【請求項３０】
前記ファイラに記憶されている全てのファイルは論理的に連続的な方式でスキャンされる請求項２３に記載の装置。
【請求項３１】
前記スキャンレポートが、前記の、前記ファイルに対する処理に関する一組のステータスデータを有する請求項２３に記載の装置。
【請求項３２】
前記ステータスデータが、前記ファイルにおけるウィルスの存在または非存在を特定する少なくとも１つのデータ要素を含んでいる請求項３１に記載の装置。
【請求項３３】
前記レポートが前記ファイラへ転送される請求項３１に記載の装置。
【請求項３４】
前記レポートが第１データベースに記憶される請求項３３に記載の装置。
【請求項３５】
その後の、前記ファイルに対するスキャンの必要性は、前記データベースが前記ファイルに関するレポートを有するか、および、前記ファイルが最後のアクセスから変更されているかに関する判断による関数である、請求項３４に記載の装置。
【請求項３６】
その後の、前記ファイルに対するスキャンの必要性は、さらなるウィルス識別データファイルが前記処理クラスタに追加されたかに関する判断による関数である、請求項３５に記載の装置。
【請求項３７】
前記レスポンスの送信とは前記ファイルを送信することである請求項２１に記載の装置。
【請求項３８】
前記レスポンスの送信が、ユーザへの前記ファイルは利用不可能である旨の通知を含む請求項２１に記載の装置。
【請求項３９】
前記の、前記リクエストに対する応答が、前記ユーザに前記スキャンレポートの部分を送ることを含んでいる請求項２１に記載の装置。
【請求項４０】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、
サーバにおいてファイルに対するリクエストを受け取るステップ、
前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送るステップ、
前記ファイルをサーバから送信しても安全であるか否かについての指摘を前記スキャン装

置から受け取るステップ、および、
前記指摘が、前記ファイルの送信が安全であるとする場合、前記ファイルを送信することで前記リクエストに応答するステップを有する、クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項４１】
前記スキャン装置が、前記ファイルがいかなるウィルスにも感染していない場合に、前記ファイルを送信しても安全であると指摘する、請求項４０に記載の方法。
【請求項４２】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項４０に記載の方法。
【請求項４３】
前記サーバがウェブサーバである、請求項４０に記載の方法。
【請求項４４】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項４０に記載の方法。
【請求項４５】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項４４に記載の方法。
【請求項４６】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、
サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するステップ、
サーバにおいてファイルに対するリクエストを受け取るステップ、
データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するステップ、
および、
データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するステップを有する、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項４７】
データベースを保持するステップがさらに、
前記スキャン装置から受け取った指摘を追跡するステップ、および、
前記ファイルに対するアクセスを追跡するステップを有する、請求項４６に記載の方法。
【請求項４８】
前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項４７に記載の方法。
【請求項４９】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項４６に記載の方法。
【請求項５０】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項４６に記載の方法。
【請求項５１】
前記サーバがウェブサーバである、請求項４６に記載の方法。
【請求項５２】

クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、
サーバより、前記サーバに接続されたスキャン装置において、前記サーバの大容量記憶装置に記憶されたファイルに対する識別子を受け取るステップ、
前記ファイルのウィルスをスキャンするステップ、および、
前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするステップを有する、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項５３】
さらに、前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正するステップを有する請求項５２に記載の方法。
【請求項５４】
前記サーバがウェブサーバである、請求項５２に記載の方法。
【請求項５５】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項５２に記載の方法。
【請求項５６】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項５５に記載の方法。
【請求項５７】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバであって、
クライアント装置との通信リンク、
大容量記憶装置、
ならびに、
リクエストされたファイルをクライアント装置に送信するための命令を実行するプロセッサを有し、
前記命令が、
（ａ）ファイルに対するリクエストを受け取るための、
（ｂ）前記ファイルのウィルスをスキャンするスキャン装置に前記ファイルに対する識別子を送信するための、
（ｃ）前記ファイルをサーバより送信しても安全であるか否かについての指摘を前記スキャン装置から受け取るための、および、
（ｄ）前記指摘が、前記ファイルは送信しても安全であると指摘していれば、前記ファイルを送信することにより、前記リクエストに応答するための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバ。
【請求項５８】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記スキャン装置が、前記ファイルは送信しても安全であると示唆する、請求項５７に記載のサーバ。
【請求項５９】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項５７に記載のサーバ。
【請求項６０】
前記サーバがウェブサーバである、請求項５７に記載のサーバ。
【請求項６１】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項５７に記載のサーバ。
【請求項６２】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項

６１に記載のサーバ。
【請求項６３】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバであって、
クライアント装置との通信リンク、
大容量記憶装置、
ならびに、
リクエストされたファイルをクライアント装置に送信するための命令を実行するプロセッサを有し、
前記命令が、
（ａ）サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するための、
（ｂ）サーバにおいてファイルに対するリクエストを受け取るための、
（ｃ）データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するための、および、
（ｄ）データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバ。
【請求項６４】
前記の、前記データベースを保持する命令がさらに、
前記スキャン装置から受け取った指摘を追跡するための、および、
前記ファイルに対するアクセスを追跡するための命令を有する、請求項６３に記載のサーバ。
【請求項６５】
前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項６４に記載のサーバ。
【請求項６６】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項６３に記載のサーバ。
【請求項６７】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項６３に記載のサーバ。
【請求項６８】
前記サーバがウェブサーバである、請求項６３に記載のサーバ。
【請求項６９】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるスキャン装置であって、
前記サーバとの通信リンク、および、
命令を実行するプロセッサを有し、
前記命令が、
（ａ）前記サーバの大容量記憶装置に記憶されたファイルに対する識別子をサーバより受け取るための、
（ｂ）前記ファイルのウィルスをスキャンするための、および、
（ｃ）前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするための、前記ファイルをサーバより送信しても安全であるか否かについての指摘を前記スキ

ャン装置から受け取るための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるスキャン装置。
【請求項７０】
さらに、前記命令が、前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正する命令を有する請求項６９に記載のスキャン装置。
【請求項７１】
前記サーバがウェブサーバである、請求項６９に記載のスキャン装置。
【請求項７２】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項６９に記載のスキャン装置。
【請求項７３】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項７２に記載のスキャン装置。
【請求項７４】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、
前記命令が、
サーバにおいてファイルに対するリクエストを受け取るステップ、
前記ファイルのウィルスをスキャンするスキャン装置に、前記ファイルに対する識別子を送信するステップ、
前記ファイルをサーバから送信しても安全であるか否かについて、前記スキャン装置からの指摘を受け取るステップ、および、
前記指摘が、前記ファイルは送信しても安全であると指摘していれば、前記ファイルを送信することにより、前記リクエストに応答するステップを含んでいる、記憶装置。
【請求項７５】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記スキャン装置が、前記ファイルは送信しても安全であると示唆する、請求項７４に記載の記憶装置。
【請求項７６】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項７４に記載の記憶装置。
【請求項７７】
前記サーバがウェブサーバである、請求項７４に記載の記憶装置。
【請求項７８】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項７４に記載の記憶装置。
【請求項７９】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項７８に記載の記憶装置。
【請求項８０】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、
前記命令が、
サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するステップ、
サーバにおいてファイルに対するリクエストを受け取るステップ、
データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するステップ、および、

データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するステップを含んでいる、記憶装置。

【請求項８１】

データベースを保持するステップがさらに、

前記スキャン装置から受け取った指摘を追跡するステップ、および、

前記ファイルに対するアクセスを追跡するステップを有する、請求項８０に記載の記憶装置。

【請求項８２】

前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項８１に記載の記憶装置。

【請求項８３】

前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項８０に記載の記憶装置。

【請求項８４】

前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項８０に記載の記憶装置。

【請求項８５】

前記サーバがウェブサーバである、請求項８０に記載の記憶装置。

【請求項８６】

クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、

前記命令が、

サーバより、前記サーバに接続されたスキャン装置において、前記サーバの大容量記憶装置に記憶されたファイルに対する識別子を受け取るステップ、

前記ファイルのウィルスをスキャンするステップ、および、

前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするステップを含んでいる、記憶装置。

【請求項８７】

前記命令がさらに、

前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正するステップを有する請求項８６に記載の記憶装置。

【請求項８８】

前記サーバがウェブサーバである、請求項８６に記載の記憶装置。

【請求項８９】

前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項８６に記載の記憶装置。

【請求項９０】

前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項８９に記載の記憶装置。

【発明の詳細な説明】

【発明の背景】

【０００１】

技術分野

本発明はネットワーク環境におけるウィルススキャンに関する。

【０００２】

関連技術

コンピュータネットワークおよびインターネットにより、エンドユーザはあらゆる種類の情報への国際的な共通基盤に基づく、新しいアクセスを享受している。情報へのアクセスは、電話線を用いてある種のコンピュータ装置をネットワークに接続するように簡便にできる。ワイヤレス通信の急増に伴い、今やユーザは事実上、どこからでもコンピュータネットワークにアクセスできる。

【０００３】

このような規模の接続性が、コンピュータウィルスの影響度を拡大している。「メリッサ(Melissa)」および「アイラブユー(I love you)」といったウィルスは、全世界のコンピュータシステムに壊滅的な打撃を与えた。ウィルス処置に要するコストはしばしば、数百万ドルにもまた数千万ドルにも達する。近年、ハンドヘルド型コンピュータ装置もまたウィルスに感染しやすいことがわかっている。

【０００４】

ウィルス保護ソフトウェアはウィルス対策において非常に効果的であり、またウィルス保護ソフトウェアはパーソナルコンピュータのような一般的なコンピュータ装置向けのものが広く流通している。しかしながら、ファイラ（データの記憶および検索に特化した装置）のような特殊なコンピュータ装置に固有の問題が存在する。市販のウィルス保護ソフトウェアは、特殊なコンピュータ装置上では、修正を加えない限り、実行されず、別のプラットフォームで稼動するようにソフトウェアを書き替えることは非常に高くつく。

【０００５】

第１の周知の方法はデータソースにおけるウィルススキャンである。特殊なコンピュータ装置によってデータが提供されようとすれば、その特殊なコンピュータ装置をスキャンする必要がある。装置内のファイルをスキャンするために、その装置用のウィルス保護ソフトウェアを記述しなければならない。

【０００６】

この第１の周知の方法は、ファイルに対してウィルススキャンをするには効果的な方法だが、幾つかの不利益を有する。先ず、特殊なコンピュータ装置を有する会社は、かなりの資産をかけてウィルス保護ソフトウェアを作りあげ、そして、現われる新しいウィルスから保護してくれるよう、データファイルを最新型に維持しなければならない。

【０００７】

そのうえ、特殊なコンピュータ装置の製造業者は、主流となっているウィルス保護ソフトウェアを作っている法人の賛助を得てカスタムアプリケーションを記述し、ライセンシーになることは可能だが、このことが、選択したアンチーウィルスソフトウェアベンダーの信頼性、ハードウェアがアップグレードされた場合の互換性に関する課題、および、多大な財務費用といった問題を引き起こしている。

【０００８】

第２の周知の、コンピュータウィルスから保護する方法は、エンドユーザに彼らのクライアント装置上でアンチーウィルスソフトウェアを実行させることである。アンチーウィルスソフトウェアは、マカフィー(McAfee)やシマンテック(Symantec)といった会社から提供されている。これらのプログラムはコンピュータのブート段階中にロードされ、バックグラウンドジョブとして動作してメモリおよびファイルを開いたり、保存したりしながら監視している。

【０００９】

この第２の周知の方法はクライアント装置の感染を阻止し、保護する上では効果的だが、幾つかの不利益を有する。これは連鎖における最終可能リンクに、検出の負担を設定している。いかなる理由があろうと、エンドユーザに到達するよりも先にウィルスを検出しなければ、ウィルスは最大の被害（ファイルの破壊、ならびに、他のコンピュータユーザおよびシステムへの拡大）を及ぼすであろうコンピュータ装置に到達する。

【００１０】

何百万というユーザへ送信されるかもしれないソースからファイルを駆除(sanitize)する

ほうが、そのファイルを送信し、そして、エンドユーザに、ファイルが感染している場合にそのファイルに対処するための用意をしておくことを期待するよりもずっとよい。エンドユーザはしばしば古いバージョンのアンチーウィルスソフトウェア、および／または、そのソフトウェアが新しく発見されたウィルスから確実に護れるようにするためのデータファイルにアップデートしていない。従って、大量配信されるポイントにおける検出を行うことがより重要である。

【００１１】

また、ハンドヘルド型コンピュータ装置もウィルスに感染しやすいが、これら装置のウィルスに対処する装備は不十分である。一般に、ハンドヘルド型コンピュータ装置はデスクトップシステムと比較して、非常に制限されたメモリリソースを有する。これらのリソースの一部分をウィルス保護に費やすと、ハンドヘルド型装置が効率的に動作する能力を厳しく制限する。情報ソースにおける信頼できるウィルススキャンが最も効率的でありかつ効果的な方法である。

【００１２】

ウィルスからの保護は絶え間の無い戦いである。新しいウィルスは毎日創出され、ウィル保護ソフトウェア製造者は新しいデータファイル（アンチーウィルスソフトウェアが使用する解決用アルゴリズム）を作り出す必要に迫られる。ファイルのソースにおいて保護することで、ウィルスはさらに効率よく、効果的に除去可能である。

【００１３】

一般にデータのセキュリティーは重要である。同程度に重要なのがエンドユーザの信用である。これは会社に先行する評判に由来し、また、ウェブコマースに従事する会社は、その評判によって生きることも死ぬこともる。それは丁度、エンドユーザがウェブベースの売買取引のために開示したクレジットカードの番号が安全であると信じているように、受信するファイルも安全であることを望んでいる。

【００１４】

従い、特殊なコンピュータ装置をスキャンして、変更、削除、または、修正の必要があるかもしれない、ウィルスおよび他の悪質なもしくは望まざる内容を調べる技術を提供することが望まれている。

【発明の概要】

【００１５】

本発明は、（ファイラのような）特殊なコンピュータ装置に対してウィルススキャンする方法およびシステムを提供する。好適な実施形態においては、ファイラは１以上の補助的コンピュータ装置と接続されており、この補助的コンピュータ装置がエンドユーザへの送信の前に、要求されたファイルをスキャンしてウィルスフリーであることを確かめる。エンドユーザがファイラからファイルを要求すると、以下のステップが実施される。第１に、要求されたファイルはエンドユーザに向けて送信する前にスキャンされなければならないかどうかを判断する。第２に、ファイラは外部コンピュータ装置の１つへのチャンネルを開き、ファイル名を送る。第３に、その外部コンピュータ装置がそのファイルを開いてスキャンする。第４に、外部コンピュータ装置がファイラへファイルスキャン操作のステータスを報告する。第５に、ファイラは、前記ステータスが送信してもよいことを示せば、ファイルをエンドユーザに送る。

【００１６】

本システムは、ファイルが修正されるか、または、新しいウィルスから保護するための新しいデータファイルが付加されないかぎり、たった一度だけファイルをウィルススキャンする必要があるという点で、非常に効率的でありまた効果的である。スキャンしたファイルのスキャンレポートは、１以上の外部コンピュータ装置、１以上のファイラに記憶されてもよく、そして、スキャンレポートのある部分はエンドユーザに送信されてもよい。

【００１７】

本発明の代替的実施形態においては、１以上のコンピュータ装置が、ファイルの圧縮や暗号化といった他の補助的アプリケーションを独立に、または、組み合わせて、実行してい

てもよい。
【好適な実施形態の詳細な説明】
【００１８】
以下の説明にて、本発明の好適な実施形態を、その好適な処理工程およびデータ構造に着目し、説明する。当業者であれば本出願を精読した後には、本発明の実施形態は１以上の一般目的もしくは特殊目的プロセッサ、または、他の、本明細書に記載の特定の処理工程およびデータ構造に適合した回路を用いて実施可能であること、ならびに、必要以上の試験または更なる発明を必要とせずに本明細書に記載の処理工程およびデータ構造を実施することができることを理解するであろう。
【００１９】
辞書編集(Lexicography)
以下の用語は、以下に説明する本発明の態様を、言及または関連する。これら用語に関する一般的な意味についての記載は、制限を加えることを目的としたものではなく、単に例示目的にすぎない。
・ウィルス－一般的に、人間が作り出したプログラムまたはコードの断片であって、コンピュータユーザの認識なしに、そのコンピュータにロードされ、そして、ユーザの意に反して実行される。たいていのウィルスは自己複製可能であり、さらに危険なタイプのウィルスにあってはネットワークを介して自身を送信し、セキュリティーシステムを迂回する能力を有する。
・クライアントおよびサーバ－一般的に、これら用語は２つの装置間の関係性について述べている。特に、クライアントおよびサーバという関係性を述べる上で必ずしも特定の物理的な装置を必要としない。
例えば、これに制限されないが、第１サーバ装置と第１の関係性を有する特定のクライアント装置が、第２クライアント装置と第２の関係性を有してサーバ装置として機能することが可能である。好適な実施形態においては一般に、比較的少数のサーバ装置が比較的多数のクライアント装置に対して情報提供を行う。
・クライアント装置およびサーバ装置－一般に、これら用語は、（ＨＴＴＰウェブクライアントおよびウェブサーバのように）クライアント－サーバ関係においてクライアント装置またはサーバ装置の役割を果たす装置をいう。いかなるクライアント装置またはサーバ装置も個別的な物理的装置でなければならないという特別な要求はない。これらは単一の装置であっても、協働する装置群であっても、装置の部分であっても、または、それらのうちのある組み合わせであってもよい。
例えば、これに制限されないが、クライアント－サーバ関係におけるクライアント装置およびサーバ装置は、実際には物理的に同一の装置とすることが可能であり、第１ソフトウェア要素群によりクライアント機能が発揮され、第２ソフトウェア要素群によりサーバ機能が発揮される。
・ウェブクライアントおよびウェブサーバ（もしくはウェブサイト）－本明細書中にて用いられる用語「ウェブクライアント」および「ウェブサーバ」（もしくは「ウェブクライアント」）は、インターネット、ワールドワイドウェブ、または、その均等物もしくはその拡張物におけるクライアント－サーバ環境において、ウェブクライアントまたはウェブサーバの役割を果たす、あらゆる装置の組み合わせまたはソフトウェアをいう。ウェブクライアントが個別的な装置でなければならないという特別な要求はない。これらは単一の装置であっても、協働する装置群であっても、装置の部分であっても、または、それらのうちのある組み合わせであってもよい（たとえば、ウェブサーバ機能を有する装置がユーザのエージェントとして動作しているように）。
【００２０】
上述のように、これらの用語に関する一般的な意味についての説明は、それらに限定することを意図したものではなく、例示を目的としている。本発明の他の、そして、さらなる適用は、これらの用語および概念の拡張も含まれているが、本出願を精読した後には、当業者にとっては明瞭であろう。これらの他の、そして、さらなる適用は本発明の範囲およ

び本発明の思想の一部であり、それらは当業者であれば別の発明または必要以上の試験をせずとも明らかである。

【００２１】

システムの要素

図１は分散化装置によるウィルススキャンのためのシステムに関するブロック図を示す。

【００２２】

システム１００はユーザ１１１と関連するクライアント装置１１０、通信ネットワーク１２０、ファイラ１３０、および、処理クラスタ１４０を有する。

【００２３】

クライアント装置１１０はプロセッサ、主メモリ、および、命令を実行するためのソフトウェア（図示せず、だが当業者であれば理解する。）を有する。クライアント装置１１０およびファイラ１３０は別個の装置として示されるが、これらが物理的に分離していることを要求しない。

【００２４】

好適な実施形態において、通信ネットワーク１２０はインターネットを含む。代替的実施形態において、通信ネットワーク１２０は、イントラネット、エクストラネット、仮想プライベートネットワーク、ダイレクト通信リンク、または、それらの組み合わせもしくは結合といった、代替的通信形態を含んでもよい。

【００２５】

通信リンク１１５はクライアント装置１１０と通信ネットワーク１２０を接続している。

【００２６】

ファイラ１３０はプロセッサ、主メモリ、命令を実行するためのソフトウェア（図示せず、だが当業者であれば理解する。）、および、大容量記憶装置１３１を有する。クライアント装置１１０およびファイラ１３０は個別の装置として示されているが、これらが個別的な装置である必要性はない。ファイラ１３０は通信ネットワーク１２０に接続されている。

【００２７】

大容量記憶装置１３１は、クライアント装置１１０からリクエスト可能な、少なくとも１つのファイル１３３を有する。

【００２８】

処理クラスタ１４０は、１以上のクラスタ装置１４１を有し、クラスタ装置１４１それぞれはプロセッサ、主メモリ、命令を実行するためのソフトウェア、および、大容量記憶装置（図示せず、だが当業者であれば理解する。）を備えている。ファイラ１３０および処理クラスタ１４０は個別の装置として示されているが、これらが個別的な装置である必要性はない。

【００２９】

好適な実施形態においては、処理クラスタ１４０は、相互通信およびファイラ１３０との直接通信可能な相互接続クラスタにおける複数のパーソナルコンピュータである。

【００３０】

クラスタリンク１３５は、処理クラスタ１４０とファイラ１３０とを接続する。クラスタリンク１３５は不均等メモリアクセス、または、イントラネット、エクストラネット、仮想プライベートネットワーク、ダイレクト通信リンク、または、それらの組み合わせもしくは結合による通信を含んでいてもよい。

【００３１】

操作方法

図２は分散化装置のウィルススキャンのためのシステムの処理流れ図である。

【００３２】

方法２００は、一組の流れのポイントおよび一組のステップを有する。システム１００が方法２００を実施する。方法２００は連続的に説明されているが、個々の要素は連動的または並列的に、非同期的にパイプライン方式で、また、その他の方式で、方法２００のス

テップを実施可能である。方法２００は、そのように指示されている場合を除き、本明細書に羅列したステップの順番と同一の順番で実施される必要性を有しない。

【００３３】

流れのポイント２００において、システム１００は方法２００を実施開始する用意ができている。

【００３４】

ステップ２０１において、ユーザ１１１はクライアント装置１１０を利用し、ファイル１３３に対するリクエストを開始する。リクエストは通信ネットワーク１２０を介してファイラ１３０に送信される。好適な実施形態においては、ファイラ１３０はウェブサーバ（図示せず、だが当業者であれば理解する。）の指示でファイル検索および記憶を実行する。

【００３５】

ステップ２０３において、ファイラ１３０はファイル１３３に対するリクエストを受け、ファイルＩＤおよびファイル１３３のパスを処理クラスタ１４０へ送信し、処理クラスタにおいて、クラスタ装置１４１のうちの１つがそれを受信する。

【００３６】

ステップ２０５において、クラスタ装置１４１はファイルＩＤおよびパスを利用してファイラ１３０の大容量記憶装置１３１のファイル１３３を開く。

【００３７】

ステップ２０７において、クラスタ装置１４１はファイル１３３のウィルススキャンを行う。好適な実施形態においては、ファイルは総当り方式(round robin fashion)で処理クラスタに課せられる(be tasked to the processing cluster 140)。代替的実施形態において、ファイルはクラスタ装置１４１によって個別的に処理されてもよく、複数のクラスタ装置１４１によって同時的にされてもよく、また、それらの組み合わせでもよい。処理クラスタ１４０内における処理の最大効率化を確保する目的で、負荷分散(load balancing)を用いてもよい。

【００３８】

パーソナルコンピュータ向けのウィルス保護ソフトを提供するベンダーは数社あるので、ファイラ１３０の操作者は使用したい製品なら何でも選んでよい。また、処理クラスタ１４０において複数ベンダーの製品を組み合わせて使用することすらかまわない。本発明の代替的実施形態においては、ファイラ１３０のあらゆるファイル１３３に対して継続的にスキャンが行われてもよい。

【００３９】

処理クラスタ１４０は高度な拡張性を有する。パーソナルコンピュータの価格は、ファイラのような専用の装置に較べて低価格であるので、このような構成は非常に望ましいものである。加えて、クラスタの構成により、クラスタ装置１４１が機能停止した場合における代理機能システム(redundant systems)を提供し、処理クラスタ内部においてフェイルオーバー(failover)およびテイクオーバー(takeover)も可能である。

【００４０】

ステップ２０９において、クラスタ装置１４１はスキャンリポートをファイラ１３０に送信する。スキャンリポートは主としてファイルが送信しても安全であるかについて報告する。別の情報についても、データベースに統計上の目的で保存してもよい（例えば、どれくらいのファイルが感染していると特定されたか、ウィルスソフトウェアはそのファイルを駆除(sanitize)できたか、または、ファイルは削除されたか）。続いて受信されたリクエストに基づく送信に際し、その前にファイル１３３をスキャンする必要があるかどうかを、前記データベースを参考にして決定してもよい。ファイル１３３が、最後にスキャンを受けて以来、変更を受けておらず、かつ、さらなるウィルスデータファイルが処理クラスタに付加されていなければ、ファイル１３３は、おそらくスキャンを受ける必要はない。つまり、ファイル１３３はさらに迅速に送信可能である。

【００４１】

他の中間的アプリケーションも、処理クラスタ１４０内において独立して実行しても、他のアプリケーションと結合して実行しても、または、その組み合わせとして実行してもよい。圧縮および暗号化ユーティリティはこれらアプリケーションの例である。ウィルススキャンを含むこれらのアプリケーションは、非常にＣＰＵに負担をかけるものであり、したがってアウトソーシングによりファイラのような専用の装置が最もすべきことを実行し、他のタスクは処理クラスタ１４１に請け負わせることが可能となり、よりよいパフォーマンスをもたらす。

【００４２】

ステップ２１１において、ファイラ１３０は、処理クラスタ１４０によるスキャンを受けて報告される利用可能性に基づいてファイル１３３をクライアント１１０に向けて送信する、または、送信しない。スキャンレポートのある部分については、ユーザへ送信してもよい。

【００４３】

本ステップにおいて、ファイル１３３に対するリクエストは受信されており、前記リクエストは処理され、そして、可能であるのならばファイル１３３は配信される。本処理は後のリクエストに対して、ステップ２０１から繰り返されてよい。

【００４４】

本発明の一般性

本発明は、ファイルに対する処理要求の別の態様に対して広範な利用可能性および一般性を有する。

【００４５】

本発明は、１以上の、以下を含むような環境に、または、それらの組み合わせに対して利用可能である。

・ファイル圧縮

・ファイル暗号化、および、

・ＣＰＵに負担をかけるタスクを専用装置から多目的コンピュータへ委託する、一般的なアウトソーシング。

【００４６】

代替的実施形態

本明細書において好適な実施形態について開示したが、本発明の概念、範囲、および、思想の範囲内においてさまざまな変形例が可能である。これらの変形例は、本出願を精読の後には当業者にとって明白である。

【図面の簡単な説明】

【００４７】

【図１】分散化された装置でのウィルススキャンのためのシステムのブロック図である。

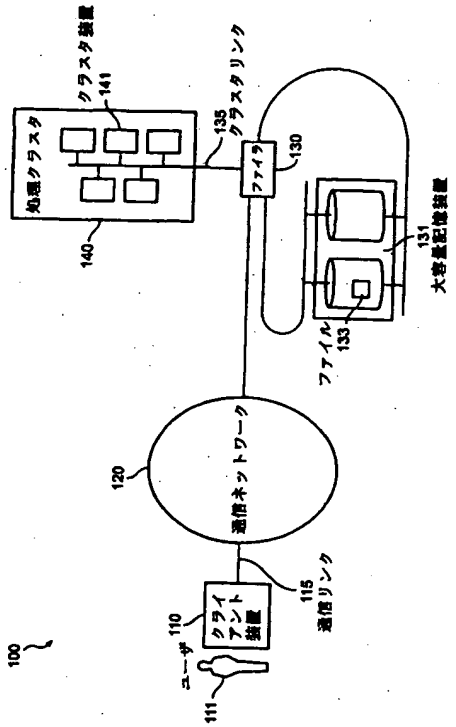
【図２】分散的ウィルススキャンのためのシステムの処理の流れ図である。

【符号の説明】

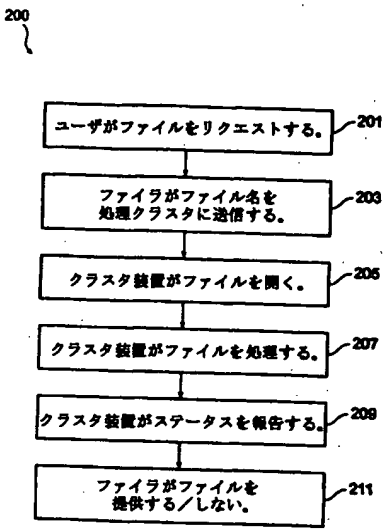
【００４８】

１００	・・ システム	１１０	・・ クライアント装置
１１１	・・ ユーザ	１１５	・・ 通信リンク
１２０	・・ 通信ネットワーク	１３０	・・ ファイラ
１３１	・・ 大容量記憶装置	１３３	・・ ファイル
１３５	・・ クラスタリンク	１４０	・・ 処理クラスタ
１４１	・・ クラスタ装置		

【図１】


クラスタ装置
141
処理クラスタ
140
135
クラスタリンク
ファイラ
130
131
大容量記憶装置
ファイル
133
120
通信ネットワーク
115
通信リンク
110
クライアント装置
ユーザ
111
100

【図２】


200
ユーザがファイルをリクエストする。
201
ファイラがファイル名を処理クラスタに送信する。
203
クラスタ装置がファイルを開く。
205
クラスタ装置がファイルを処理する。
207
クラスタ装置がステータスを報告する。
209
ファイラがファイルを提供する／しない。
211

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/44862 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/US01/46588

(22) International Filing Date:
30 November 2001 (30.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/728,701 1 December 2000 (01.12.2000) US

(71) Applicant: NETWORK APPLIANCE, INC. [US/US]; 495 East Java Drive, Sunnyvale, CA 94089 (US).

(72) Inventor: MUHLESTEIN, Mark; 5831 E. Placita Alta Reposa, Tucson, AZ 85750 (US).

(74) Agent: SWERNOFSKY, Steven, A.; Swernofsky Law Group, P.O. Box 390013, Mountain View, CA 94039-0013 (US).

(81) Designated States (national): CA, JP.

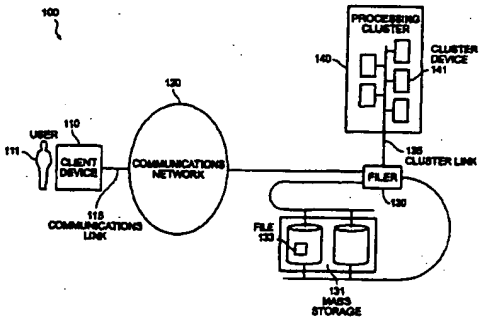
(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Declarations under Rule 4.17:
— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations
— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:
— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: DECENTRALIZED APPLIANCE VIRUS SCANNING



(57) Abstract: The invention provides a method and system for scanning specialized computing devices for viruses. In a preferred embodiment, a filer is connected to one or more supplementary computing devices that scan requested files to ensure they are virus free prior to delivery to end users. When an end user requests a file the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one of the external computing devices and sends the filename. Third, the external computing device opens the file and scans it. Fourth, the external computing device notifies the filer the results of the file scan operation. Fifth, the filer sends the file to the end user provided the status indicates it may do so.

WO 02/44862 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DECENTRALIZED APPLIANCE VIRUS SCANNING

Background of the Invention

1. *Field of the Invention*

This invention relates to virus scanning in a networked environment.

2. *Related Art*

Computer networking and the Internet in particular offer end users unprecedented access to information of all types on a global basis. Access to information can be as simple as connecting some type of computing device using a standard phone line to a network. With the proliferation of wireless communication, users can now access computer networks from practically anywhere.

Connectivity of this magnitude has magnified the impact of computer viruses. Viruses such as "Melissa" and "I love you" had a devastating impact on computer systems worldwide. Costs for dealing with viruses are often measured in millions and tens of millions of dollars. Recently it was shown that hand-held computing devices are also susceptible to viruses.

Virus protection software can be very effective in dealing with viruses, and virus protection software is widely available for general computing devices such as personal computers. There are, however, problems unique to specialized computing devices, such as filers (devices dedicated to storage and retrieval of data). Off-the-shelf virus protection software will not run on a specialized computing device unless it is modified to do so, and it can be very expensive to rewrite software to work on another platform.

A first known method is to scan for viruses at the data source. When the data is being provided by a specialized computing device the specialized computing device must be scanned. Device-specific virus protection software must be written in order to scan the files on the device.

While this first known method is effective in scanning files for viruses, it suffers from several drawbacks. First, a company with a specialized computing device would have to dedicate considerable resources to creating virus protection software and maintaining up-to-date data files that protect against new viruses as they emerge.

Additionally, although a manufacturer of a specialized computing device could enlist the assistance of a company that creates mainstream virus protection software to write the custom application and become a licensee this would create other problems, such as reliance on the chosen vendor of the anti-virus software, compatibility issues when hardware upgrades are effected, and a large financial expense.

A second known method for protecting against computer viruses is to have the end user run anti-virus software on their client device. Anti-virus software packages are offered by such companies as McAfee and Symantec. These programs are loaded during the boot stage of a computer and work as a background job monitoring memory and files as they are opened and saved.

While this second known method is effective at intercepting and protecting the client device from infection, it suffers from several drawbacks. It places the burden of detection at the last possible link in the chain. If for any reason the virus is not detected prior to reaching the end user it is now at the computing device where it will do the most damage (corrupting files and spreading to other computer users and systems).

It is much better to sanitize a file at the source from where it may be delivered to millions of end users rather than deliver the file and hope that the end user is prepared to deal with the file in the event the file is infected. End users often have older versions of anti-virus software and/or have not updated the data files that ensure the software is able to protect against newly discovered viruses, thus making detection at the point of mass distribution even more critical.

Also, hand-held computing devices are susceptible to viruses, but they are poorly equipped to handle them. Generally, hand-held computing devices have very limited memory resources compared to desktop systems. Dedicating a portion of these resources to virus protection severely limits the ability of the hand-held device to perform effectively. Reliable virus scanning at the information source is the most efficient and effective method.

Protecting against viruses is a constant battle. New viruses are created everyday requiring virus protection software manufacturers to come up with new data files (solution algorithms used by anti-virus applications). By providing protection at the source of the file, viruses can be eliminated more efficiently and effectively.

Security of data in general is important. Equally important is the trust of the end user. This comes from the reputation that precedes a company, and companies that engage in web commerce often live and die by their reputation. Just like an end user trusts that the credit card number they have just disclosed for a web-based sales transaction is secure they want files they receive to be just as secure.

Accordingly, it would be desirable to provide a technique for scanning specialized computing devices for viruses and other malicious or unwanted content that may need to be changed, deleted, or otherwise modified.

Summary of the Invention

The invention provides a method and system for scanning specialized computing devices (such as filers) for viruses. In a preferred embodiment, a filer is connected to one or more supplementary computing devices that scan requested files to ensure they are virus free prior to delivery to end users. When an end user requests a file from the filer the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one of the external computing devices and sends the filename. Third, the external computing device opens the file and scans it. Fourth, the external computing device notifies the filer the status of the file scan operation. Fifth, the filer sends the file to the end user provided the status indicates it may do so.

This system is very efficient and effective as a file needs only to be scanned one time for a virus unless the file has been modified or new data files that protect against new viruses have been added. Scan reports for files that have been scanned may be stored in one or more of the external computing devices, in one or more filers, and some portion of a scan report may be delivered to end users.

In alternative embodiments of the invention one or more of the external computing devices may be running other supplementary applications, such as file compression and encryption, independently or in some combination.

Brief Description of the Drawings

Figure 1 shows a block diagram of a system for decentralized appliance virus scanning.

Figure 2 shows a process flow diagram for a system for decentralized virus scanning

Detailed Description of the Preferred Embodiment

In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. Those skilled in the art would recognize after perusal of this application that embodiments of the invention can be implemented using one or more general purpose processors or special purpose processors or other circuits adapted to particular process steps and data structures described herein, and that implementation of the process steps and data structures described herein would not require undue experimentation or further invention.

Lexicography

The following terms refer or relate to aspects of the invention as described below. The descriptions of general meanings of these terms are not intended to be limiting, only illustrative.

- Virus – in general, a manmade program or piece of code that is loaded onto a computer without the computer user's knowledge and runs against their wishes. Most viruses can also replicate themselves, and the more dangerous types of viruses are capable of transmitting themselves across networks and bypassing security systems.

- client and server — in general, these terms refer to a relationship between two devices, particularly to their relationship as client and server, not necessarily to any particular physical devices.

  For example, but without limitation, a particular client device in a first relationship with a first server device, can serve as a server device in a second relationship with a second client device. In a preferred embodiment, there are

generally a relatively small number of server devices servicing a relatively larger number of client devices.

- **client device and server device** — in general, these terms refer to devices taking on the role of a client device or a server device in a client-server relationship (such as an HTTP web client and web server). There is no particular requirement that any client devices or server devices must be individual physical devices. They can each be a single device, a set of cooperating devices, a portion of a device, or some combination thereof.

  For example, but without limitation, the client device and the server device in a client-server relation can actually be the same physical device, with a first set of software elements serving to perform client functions and a second set of software elements serving to perform server functions.

- **web client** and **web server** (or **web site**) — as used herein the terms "web client" and "web server" (or "web site") refer to any combination of devices or software taking on the role of a web client or a web server in a client-server environment in the internet, the world wide web, or an equivalent or extension thereof. There is no particular requirement that web clients must be individual devices. They can each be a single device, a set of cooperating devices, a portion of a device, or some combination thereof (such as for example a device providing web server services that acts as an agent of the user).

As noted above, these descriptions of general meanings of these terms are not intended to be limiting, only illustrative. Other and further applications of the invention, including extensions of these terms and concepts, would be clear to those of ordinary skill in the art after perusing this application. These other and further applications are part of the scope and spirit of the invention, and would be clear to those of ordinary skill in the art, without further invention or undue experimentation.

System Elements

Figure 1 shows a block diagram of a system for decentralized appliance virus scanning.

A system 100 includes a client device 110 associated with a user 111, a communications network 120, a filer 130, and a processing cluster 140.

The client device 110 includes a processor, a main memory, and software for executing instructions (not shown, but understood by one skilled in the art). Although the client device 110 and filer 130 are shown as separate devices there is no requirement that they be physically separate.

In a preferred embodiment, the communication network 120 includes the Internet. In alternative embodiments, the communication network 120 may include alternative forms of communication, such as an intranet, extranet, virtual private network, direct communication links, or some other combination or conjunction thereof.

A communications link 115 operates to couple the client device 110 to the communications network 120.

The filer 130 includes a processor, a main memory, software for executing instructions (not shown, but understood by one skilled in the art), and a mass storage 131. Although the client device 110 and filer 130 are shown as separate devices there is no requirement that they be separate devices. The filer 130 is connected to the communications network 120.

The mass storage 131 includes at least one file 133 that is capable of being requested by a client device 110.

The processing cluster 140 includes one or more cluster device 141 each including a processor, a main memory, software for executing instructions, and a mass storage (not shown but understood by one skilled in the art). Although the filer 130 and the processing cluster 140 are shown as separate devices there is no requirement that they be separate devices.

In a preferred embodiment the processing cluster 140 is a plurality of personal computers in an interconnected cluster capable of intercommunication and direct communication with the filer 130.

The cluster link 135 operates to connect the processing cluster 140 to the filer 130. The cluster link 135 may include non-uniform memory access (NUMA), or communication via an intranet, extranet, virtual private network, direct communication links, or some other combination or conjunction thereof.

Method of Operation

Figure 2 shows a process flow diagram for a system for decentralized appliance virus scanning.

A method 200 includes a set of flow points and a set of steps. The system 100 performs the method 200. Although the method 200 is described serially, the steps of the method 200 can be performed by separate elements in conjunction or in parallel, whether asynchronously, in a pipelined manner, or otherwise. There is no particular requirement that the method 200 be performed in the same order in which this description lists the steps, except where so indicated.

At a flow point 200, the system 100 is ready to begin performing the method 200.

At a step 201, a user 111 utilizes the client device 110 to initiate a request for a file 133. The request is transmitted to the filer 130 via the communications network 120. In a preferred embodiment the filer 130 is performing file retrieval and storage at the direction of a web server (not shown but understood by one skilled in the art).

At a step 203, the filer 130 receives the request for the file 133 and sends the file ID and path of the file 133 to the processing cluster 140 where it is received by one of the cluster device 141.

At a step 205, the cluster device 141 uses the file ID and path to open the file 133 in the mass storage 131 of the filer 130.

At a step 207, the cluster device 141 scans the file 133 for viruses. In a preferred embodiment, files are tasked to the processing cluster 140 in a round robin fashion. In alternative embodiments files may be processed individually by a cluster device 141, by multiple cluster device 141 simultaneously, or some combination thereof. Load balancing may be used to ensure maximum efficiency of processing within the processing cluster 140.

There are several vendors offering virus protection software for personal computers, thus the operator of the filer 130 may choose whatever product they would like to use. They may even use combinations of vendors' products in the processing cluster 140. In an alternative embodiment of the invention, continual scanning of every file 133 on the filer 130 may take place.

The processing cluster 140 is highly scalable. The price of personal computers is low compared to dedicated devices, such as filers, therefore this configuration is very desirable. Additionally, a cluster configuration offers redundant systems availability in case a cluster device 141 fails – failover and takeover is also possible within the processing cluster.

At a step 209, the cluster device 141 transmits a scan report to the filer 130. The scan report primarily reports whether the file is safe to send. Further information may be saved for statistical purposes (for example, how many files have been identified as infected, was the virus software able to sanitize the file or was the file deleted) to a database. The database may be consulted to determine whether the file 133 needs to be scanned before delivery upon receipt of a subsequent request. If the file 133 has not changed since it was last scanned and no additional virus data files have been added to the processing cluster, the file 133 probably does not need to be scanned. This means the file 133 can be delivered more quickly.

Other intermediary applications may also run separately, in conjunction with other applications, or in some combination thereof within the processing cluster 140. Compression and encryption utilities are some examples of these applications. These types of applications, including virus scanning, can be very CPU intensive, thus outsourcing can yield better performance by allowing a dedicated device like a filer to do what it does best and farm out other tasks to the processing cluster 140.

At a step 211, the filer 130 transmits or does not transmit the file 133 to the client 110 based on its availability as reported following the scan by the processing cluster 140. Some portion of the scan report may also be transmitted to the user.

At this step, a request for a file 133 has been received, the request has been processed, and if possible a file 133 has been delivered. The process may be repeated at step 201 for subsequent requests.

Generality of the Invention

The invention has wide applicability and generality to other aspects of processing requests for files.

The invention is applicable to one or more of, or some combination of, circumstances such as those involving:

- file compression;
- file encryption; and
- general outsourcing of CPU intensive tasks from dedicated appliances to general purpose computers.

Alternative Embodiments

Although preferred embodiments are disclosed herein, many variations are possible which remain within the concept, scope, and spirit of the invention, and these variations would become clear to those skilled in the art after perusal of this application.

Claims

1. A method for operating a filer including the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes at least one of the following: (1) searching for one or more recognizable patterns of data within said object, (2) compressing said object, and (3) encrypting said object;

responding to said request, wherein said step of responding includes delivery of a response to said user.

2. The method of claim 1, wherein said request is in an electronic form.

3. The method of claim 1, wherein said object is a file.

4. The method of claim 3, wherein said step of processing said request further includes the steps of:

creating an access path from said filer to a processing cluster;

processing said file in said processing cluster; and

generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

5. The method of claim 4, wherein said step of creating an access path includes sending the ID and path of said file from said filer to said processing cluster.

6. The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access.

7. The method of claim 5, wherein said step of sending is accomplished using a communications network.

8. The method of claim 5, wherein said step of sending is accomplished using a direct connection.

9. The method of claim 4, wherein said step of processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

10. The method of claim 4, wherein said step of processing of said file is accomplished in parts by more than one device in said processing cluster.

11. The method of claim 4, wherein all files stored on said filer are scanned in a logical continuous manner.

12. The method of claim 4, wherein said scan report contains a set of status data relating to said processing of said file.

13. The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

14. The method of claim 13, wherein said report is transferred to said filer.

15. The method of claim 14, wherein said report is stored in a first database.

16. The method of claim 15, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

17. The method of claim 16, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

18. The method of claim 1, wherein said delivery of a response is said file.

19. The method of claim 1, wherein said delivery of a response includes notification to said user that said file is unavailable.

20. The method of claim 1, wherein said step of responding to said request includes sending said user a copy of said scan report.

21. An apparatus for operating a filer including:

means for receiving at a first location a request from a user for an object;

means for processing said request at a second location, wherein said means for processing includes at least one of the following: (1) means for searching for one or more recognizable patterns of data within said object, (2) means for compressing said object, and (3) means for encrypting said object:

means for responding to said request, wherein said means for responding includes delivery of a response to said user.

22. The apparatus of claim 21, wherein said object is a file.

23. The apparatus of claim 22, wherein said means for processing said request further includes:

means for creating an access path from said filer to a processing cluster;

means for processing said file in said processing cluster; and

means for generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

24. The apparatus of claim 23, wherein said means for creating an access path includes means for sending the ID and path of said file from said filer to said processing cluster.

25. The apparatus of claim 24, wherein said sending is accomplished using non-uniform memory access.

26. The apparatus of claim 24, wherein said sending is accomplished using a communications network.

27. The apparatus of claim 24, wherein said sending is accomplished using a direct connection.

28. The apparatus of claim 23, wherein said processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

29. The apparatus of claim 23, wherein said processing of said file is performed on atomic units of said file by more than one device in said processing cluster.

30. The apparatus of claim 23, wherein all files stored on said filer are scanned in a logical continuous manner.

31. The apparatus of claim 23, wherein said scan report contains a set of status data relating to said processing of said file.

32. The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

33. The apparatus of claim 31, wherein said report is transferred to said filer.

34. The apparatus of claim 33, wherein said report is stored in a first database.

35. The apparatus of claim 34, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

36. The apparatus of claim 35, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

37. The apparatus of claim 21, wherein said delivery of a response is delivery of said file.

38. The apparatus of claim 21, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable.

39. The apparatus of claim 21, wherein said responding to said request includes sending said user some portion of said scan report.

40. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

41. A method as in claim 40, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

42. A method as in claim 40, wherein the request is received from and the file is sent to a client device.

43. A method as in claim 40, wherein the server is a web server.

44. A method as in claim 40, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

45. A method as in claim 44, wherein the cluster of devices is a cluster of interconnected personal computers.

46. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

47. A method as in claim 46, wherein maintaining the database further comprises the steps of:

tracking received indications from the scanning device; and

tracking accesses to the file.

48. A method as in claim 47, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

49. A method as in claim 46, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

50. A method as in claim 46, wherein the request is received from and the file is sent to a client device.

51. A method as in claim 46, wherein the server is a web server.

52. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

53. A method as in claim 52, further comprising the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

54. A method as in claim 52, wherein the server is a web server.

55. A method as in claim 52, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

56. A method as in claim 55, wherein the cluster of devices is a cluster of interconnected personal computers.

57. A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to receive a request for a file, (b) to send an identifier for the file to a scanning device that scans the file for viruses, (c) to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and (d) to respond to the request by sending the file if the indication is that the file is safe to send.

58. A server as in claim 57, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

59. A server as in claim 57, wherein the request is received from and the file is sent to a client device.

60. A server as in claim 57, wherein the server is a web server.

61. A server as in claim 57, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

62. A server as in claim 61, wherein the cluster of devices is a cluster of interconnected personal computers.

63. A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to maintain a database that indicates if files served by a server are safe to send from the server, (b) to receive a request at the server for a file, (c) if the database indicates that the file is safe to send, to respond to the request by sending the file, and (d) if the database does not indicate that the file is safe to send, then to send an identifier for the file to a scanning device that scans the file for viruses, to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and to respond to the request by sending the file if the indication is that the file is safe to send.

64. A server as in claim 63, wherein the instructions to maintain the database further comprise instructions to track received indications from the scanning device, and to track accesses to the file.

65. A server as in claim 64, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

66. A server as in claim 63, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

67. A server as in claim 63, wherein the request is received from and the file is sent to a client device.

68. A server as in claim 63, wherein the server is a web server.

69. A scanning device that attempts to provide virus protection for a server in a client-server environment, comprising:

a communication link to the server; and

a processor that executes instructions, the instructions including instructions (a) to receive from the server an identifier for a file stored on mass storage for the server, (b) to scan the file for viruses, and (c) to report an indication to the server as to whether or not the file is infected.

70. A scanning device as in claim 69, wherein the instructions further comprise instructions to change, delete, or otherwise modify the file based on a result of scanning the file for viruses.

71. A scanning device as in claim 69, wherein the server is a web server.

72. A scanning device as in claim 69, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

73. A scanning device as in claim 72, wherein the cluster of devices is a cluster of interconnected personal computers.

74. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

75. Storage as in claim 74, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

76. Storage as in claim 74, wherein the request is received from and the file is sent to a client device.

77. Storage as in claim 74, wherein the server is a web server.

78. Storage as in claim 74, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

79. Storage as in claim 78, wherein the cluster of devices is a cluster of interconnected personal computers.

80. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

81. Storage as in claim 80, wherein maintaining the database further comprises the steps of:

tracking received indications from the scanning device; and

tracking accesses to the file.

82. Storage as in claim 81, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

83. Storage as in claim 80, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

84. Storage as in claim 80, wherein the request is received from and the file is sent to a client device.

85. Storage as in claim 80, wherein the server is a web server.

86. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

87. Storage as in claim 86, wherein the instructions further comprise the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

88. Storage as in claim 86, wherein the server is a web server.

89. Storage as in claim 86, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

90. Storage as in claim 89, wherein the cluster of devices is a cluster of interconnected personal computers.

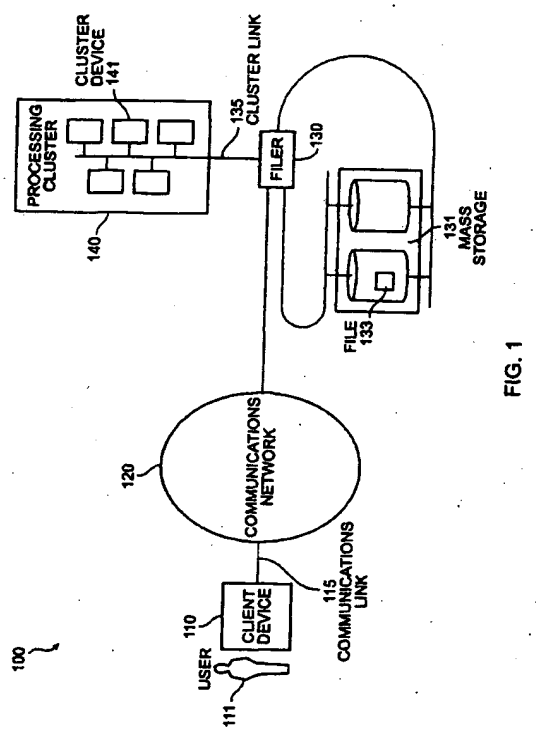

CLUSTER DEVICE 141
135 CLUSTER LINK
PROCESSING CLUSTER
140
FILER
130
131 MASS STORAGE
FILE 133
120
COMMUNICATIONS NETWORK
115 COMMUNICATIONS LINK
110
CLIENT DEVICE
USER
111
100

FIG. 1

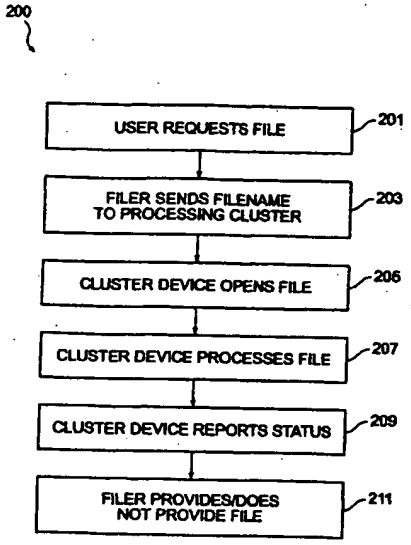

200
USER REQUESTS FILE
201
FILER SENDS FILENAME TO PROCESSING CLUSTER
203
CLUSTER DEVICE OPENS FILE
205
CLUSTER DEVICE PROCESSES FILE
207
CLUSTER DEVICE REPORTS STATUS
209
FILER PROVIDES/DOES NOT PROVIDE FILE
211

FIG. 2

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/044862 A3

(51) International Patent Classification⁷: G06F 7/00, 11/34

(21) International Application Number: PCT/US01/46683

(22) International Filing Date:
30 November 2001 (30.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/728,701 1 December 2000 (01.12.2000) US

(71) Applicant: NETWORK APPLIANCE, INC. [US/US]; 495 East Java Drive, Sunnyvale, CA 94089 (US).

(72) Inventor: MUHLESTEIN, Mark; 5831 E. Placita Alta Reposa, Tucson, AZ 85750 (US).

(74) Agent: SWERNOFSKY, Steven, A.; Swernofsky Law Group, P.O. Box 390013, Mountain View, CA 94039-0013 (US).

(81) Designated States (national): CA, JP.

(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

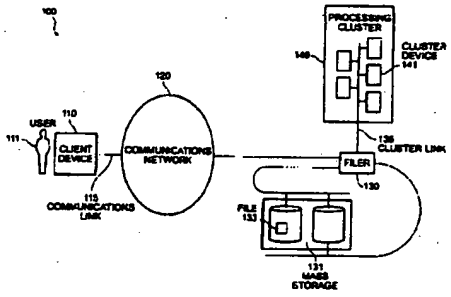
Declarations under Rule 4.17:
— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations
— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:
— with international search report

(88) Date of publication of the international search report:
30 May 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DECENTRALIZED APPLIANCE VIRUS SCANNING



(57) Abstract: The invention provides a method and system for scanning specialized computing devices for viruses. In a preferred embodiment, a filer (130) is connected to one or more supplementary computing devices (140) that scan requested files to ensure they are virus free prior to delivery to end users. When an end user (111) requests a file the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one (141) of the external computing devices and sends (203) the filename. Third, the external computing device opens (205) the file and scans (207) it. Fourth, the external computing device notifies the filer the results of the file scan operation. Fifth, the filer sends (211) the file to the end user provided the status indicates it may do so.

WO 02/044862 A3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/40888

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 7/00, 11/34
US CL. : 713/188, 200, 201; 707/6
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/188, 200, 201; 707/6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST
search terms: computer, virus, database, server, filer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,088,803 A (TSO et al.) 11 July 2000, Abstract, Figures 1 and 2.	1, 2 , 3, 18-21 and 37-39 --- 4-17, 22-36 and 40-90
Y	US 5,392,446 A (TOWER et al.) 21 February 1995, Abstract, Fig. 2, columns 1-5.	4-17, 22-36 and 40-90
Y	US 6,101,558 A (ATSUNOMIYA et al) 08 August 2000, Abstract, Figure 1.	4-17, 22-36 and 40-90
Y	US 5,918,008 A (TOGAWA et al.) 29 June 1999, Abstract and Figures.	46-51, 53-68 and 80-85.

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 JULY 2002	07 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LY V. HUA Telephone No. (703) 305-9686

Form PCT/ISA/210 (second sheet) (July 1998)*

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.